UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

IN THE MATTER OF THE SEARCH OF MULTIPLE ELECTRONIC DEVICES MORE FULLY DESCRIBED IN ATTACHMENT A

Case No. 20-144-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A for full description of multiple electronic devices to be searched.

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

electronic data stored on multiple electronic devices described in Attachment A, currently in the possession of the FBI, Philadelphia Office.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 USC Section 841(a)(1)	Possession with intent to distribute controlled substances
21 USC Section 846	Conspiracy to distribute controlled substances

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

William Wickman, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: January 31, 2020

Judge's signature

City and state: Philadelphia, Pennsylvania

RICHARD A. LLORET, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE XS, IMEI 357269098356892; APPLE IPHONE 6, IMEI 352015079785574; LTS DIGITAL VIDEO RECORDER, SERIAL NUMBER 8401804ZUX01512; APPLE IPHONE 6S, IMEI 354956075078167; APPLE IPHONE 6, IMEI 352013079368335; APPLE IPHONE 6, IMEI 356148093039706; APPLE IPHONE 6, IMEI 355786075130026; BLACKBERRY 9360 CURVE, IMEI 351602056110362; ALCATEL A521L, IMEI 014262000754309; SAMSUNG SM-J400M, IMEI 352820102574634; APPLE MACBOOK AIR, SERIAL NUMBER C02J5TEDDRVC; HP CHROMEBOOK, SERIAL NUMBER 8CG7521XZR; CURRENTLY LOCATED AT THE PHILADELPHIA FIELD OFFICE OF THE FEDERAL BUREAU OF INVESTIGATION	Case No. 20-144-M

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH

I, William R. Wickman, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since 2005. I am currently assigned to the Philadelphia Division Safe Streets Violent Gang Task

Force and have been in that assignment since 2008. During my tenure with the FBI, I have participated in numerous narcotics investigations and have become familiar with, among other things, the manner in which illegal drugs are imported and distributed; the method of payments for such drugs; and the efforts of persons involved in such activities to avoid detection by law enforcement. Over the course of these investigations I have conducted interviews of witnesses, victims and suspects, participated in physical and electronic surveillance, utilized pen registers and trap and trace devices, applied for and received numerous search and seizure warrants and arrest warrants. I have participated in searches authorized by consent, search warrants and other legal grounds, for residences, businesses, electronic devices and vehicles for the purpose of obtaining evidence.

3. I am an FBI certified Forensic Examiner and a member of the FBI's Computer Analysis Response Team ("CART"). As a Forensic Examiner and member of CART, I have received extensive specialized training concerning the seizure, examination and exploitation of digital evidence, to include cellular telephones and computers.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE PROPERTY TO BE EXAMINED

5. The property to be searched, collectively hereinafter "the Devices", is:

a. A rose gold Apple iPhone XS, IMEI 357269098356892, hereinafter the "iPhone #1", which was seized from JUNIOR SORIANO FELIX subsequent to his arrest. The device is passcode protected and additional identifying information is not available in the phone's current state. iPhone #1 is currently located at the FBI Philadelphia Field Office.

b. A silver Apple iPhone 6, IMEI 352015079785574, hereinafter the "iPhone #2", which was seized from JUNIOR SORIANO FELIX subsequent to his arrest. The device is passcode protected and additional identifying information is not available in the phone's current state. iPhone #2 is currently located at the FBI Philadelphia Field Office.

c. An LTS digital video recorder, model LTD8304K-ET, serial number 8401804ZUX01512, hereinafter the "DVR", which was seized subsequent to the execution of a Commonwealth of Pennsylvania search warrant at 1808 Afton Street, Philadelphia, Pennsylvania. The DVR is currently located at the FBI Philadelphia Field Office.

d. A silver Apple iPhone 6S, IMEI 354956075078167, hereinafter the "iPhone #3", which was seized from the center console of a Buick Enclave belonging to YANTOHINC HERRERA. The device is passcode protected and additional identifying information is not available in the phone's current state. iPhone #3 is currently located at the FBI Philadelphia Field Office.

e. A silver Apple iPhone 6, IMEI 352013079368335, hereinafter the "iPhone #4", which was seized from 7131 Beech Tree Drive, Elkins Park, PA, subsequent to the execution of a search warrant. iPhone #4 is currently located at the FBI Philadelphia Field Office.

f. A gold Apple iPhone 6, IMEI 356148093039706, hereinafter the "iPhone #5", which was seized from 7131 Beech Tree Drive, Elkins Park, PA, subsequent to the execution of a search warrant. iPhone #5 is currently located at the FBI Philadelphia Field Office.

g. A silver Apple iPhone 6, IMEI 355786075130026, hereinafter the "iPhone #6", which was seized from 7131 Beech Tree Drive, Elkins Park, PA, subsequent to the execution of a search warrant. The device is passcode protected and additional identifying information is not available in the phone's current state. iPhone #6 is currently located at the FBI Philadelphia Field Office.

h. A white Blackberry 9360 Curve, IMEI 351602056110362, hereinafter the "Blackberry", which was seized from 7131 Beech Tree Drive, Elkins Park, PA, subsequent to the execution of a search warrant. The Blackberry is currently located at the FBI Philadelphia Field Office.

i. An Alcatel A521L cell phone, IMEI 014262000754309, hereinafter the "Alcatel", which was seized from 7131 Beech Tree Drive, Elkins Park, PA, subsequent to the execution of a search warrant. The Alcatel is currently located at the FBI Philadelphia Field Office.

j. An Apple MacBook Air, serial number C02J5TEDDRVC, hereinafter the "MacBook", which was seized from 7131 Beech Tree Drive, Elkins Park, PA, subsequent to the execution of a search warrant. The MacBook is currently located at the FBI Philadelphia Field Office.

k. A HP Chromebook, serial number 8CG7521XZR, hereinafter the "Chromebook", which was seized from 7131 Beech Tree Drive, Elkins Park, PA, subsequent to the execution of a search warrant. The Chromebook is currently located at the FBI Philadelphia Field Office.

l. A Samsung SM-J400M cell phone, IMEI 352820102574634, hereinafter the, "Samsung", which was seized from MYRIAM SEVILLA on January 11, 2020

subsequent to her arrest. The Samsung is currently located at the FBI Philadelphia Field Office.

6. The applied-for warrant would authorize the forensic examination of the Devices, items listed in paragraph 5(a) through 5(k), for the purpose of identifying electronically stored data particularly described in Attachment B.

FACTS ESTABLISHING PROBABLE CAUSE

7. In October 2015, YANTHONIC HERRERA was arrested during a joint FBI/DEA/Philadelphia Police Department investigation. Agents and officers had conducted controlled purchases of a large amount of bulk heroin from HERREA using a confidential informant. Further investigation led to issuance of search warrants for HERRERA's residence which resulted in the seizure of in excess of one kilogram of heroin.

8. HERRERA was indicted in the District of Delaware and charged with possession of heroin. HERRERA pleaded guilty and was sentenced to nine months imprisonment and a term of 60 months supervised release.

9. In the summer of 2018, investigators received information from a confidential informant[1] that HERRERA and others were again involved in the distribution of heroin in and around the Philadelphia area. Investigators conducted numerous surveillances and were able to identify multiple properties at which members of the HERRERA organization were often observed. One of these properties, 1808 Afton Street, Philadelphia, PA, was a location where members of the HERRERA organization often congregated. Fixed surveillance was established

[1] The confidential informant has provided consistently reliable information on multiple subjects of FBI investigations. The confidential informant has provided information which has led to multiple seizures of bulk heroin and Fentanyl as well as multiple arrests and convictions in Federal court.

at 1808 Afton Street in October 2018 in an effort to gather further intelligence about HERRERA and his associates.

10. It was determined that 1808 Afton Street was the residence of JUNIOR SORIANO FELIX, a known associate of HERRERA. Information provided by the confidential informant indicated that HERRERA, FELIX and others were involved in distribution of heroin in and around the Philadelphia area. However, the confidential informant was not in a position to specifically describe each individual's role in the organization.

11. Continued surveillance and checks of law enforcement databases identified HERRERA's primary residence, which he shared with his girlfriend, MYRIAM SEVILLA, as 7131 Beech Tree Drive, Elkins Park, Pennsylvania. In addition, it was determined the HERRERA and his girlfriend, MYRIAM SEVILLA, often drove a gold Buick Enclave SUV bearing Pennsylvania registration KZM-0306.

12. On July 21, 2019, an individual, herein referred to as "the victim," filed a complaint at the Philadelphia Police Department's Northeast Detective Division. The victim stated that he had been held against his will, beaten and threatened by a group of five males. The victim was familiar with some of the males but could only identify the males by their first names or nick names.

13. The victim stated that on Saturday, July 20, 2019, he had been asked by an associate, known only to the victim as "MAX", to hang out and smoke marijuana together. The victim agreed to do so and was picked up by a Buick Enclave driven by "JOHN". The victim stated the Buick Enclave was unique as it had been badly keyed numerous times all over the sides of the vehicle. Also in the Buick Enclave were MAX, JUNIOR, and MANNY. While in the Buick, JUNIOR asked for the victim's cell phone which the victim provided to JUNIOR.

JUNIOR never returned the victim's cell phone. The victim was driven to a residence in Northeast Philadelphia and led into the rear of the property. The victim believed the property was located in the 1700 block of Afton Street in Philadelphia.

14. Once inside the property, the victim was told by JOHN to sit in a chair and was then shown a video, which the victim deduced was surveillance footage from a residence. JOHN accused the victim of having taken part in a robbery and demanded to know what had happened to the "stuff". The victim believes that drugs were stolen out the house and JOHN owned the house. The victim denied any knowledge of the robbery and was then punched in the head and body by the four males who had brought him to the house and one additional male who the victim knows only as "BLACK." The victim was then taped to the chair. When the victim continued to deny any knowledge of the robbery. JOHN and others then threatened to cut off the victim's arms and legs and kill the victim's family. JUNIOR then produced a handgun, cycled the slide and pointed it at the victim's head. The victim continued to deny any knowledge of the robbery. $200 was taken from the victim's front pocket and never returned.

15. Eventually JOHN and JUNIOR left the residence. The victim stated MAX, MANNY and BLACK removed the duct tape from the victim and relocated the victim to the main level of the house. MAX and MANNY then exited the residence to smoke cigarettes and BLACK was left to watch the victim. The victim asked to use the bathroom and BLACK allowed him to do so. As the victim was returning from the bathroom the victim observed that BLACK had fallen asleep. The victim then fled the house through the basement and escaped to his girlfriend's residence.

16. Detectives from Northeast Detectives drove the victim to the 1700 block of Afton Street and after canvassing the area the victim stated that he believed the house was actually

located on the 1800 block of Afton Street. Upon arriving on the 1800 block of Afton Street the victim identified 1808 Afton Street as the house where he had been held against his will.

17. On July 22, 2019, your affiant learned of the incident at 1808 Afton Street. Agents reviewed fixed surveillance video from the weekend and observed activity that was consistent with the victim's statement. Investigators believed that the individual identified by the victim as JOHN was in fact YANTHONIC HERRERA and JUNIOR was in fact JUNIOR SORIANO FELIX. MAX was believed to be MAXWELL GOMEZ, an associate and relative of HERRERA.

18. Based on the information investigators provided to Northeast Detectives, Detectives showed the victim three separate photo lineups. Photos of YANTHONIC HERREA, JUNIOR SORIANO FELIX and MAXWELL GOMEZ were included on separate lineups. The victim positively identified YANTHONIC HERRERA and JUNIOR SORIANO FELIX as having been involved in the detention and beating of the victim.

19. Based upon the positive identification of YANTHONIC HERRERA and JUNIOR SORIANO FELIX, Northeast detectives obtained a search warrant for 1808 Afton Street and planned to arrest HERRERA, FELIX and GOMEZ if they could be located.

20. On the morning of July 23, 2019, the FBI Safe Streets Task Force established surveillance of 1808 Afton Street, 7131 Beech Tree Drive and 5945 North Lawrence Street (the residence of GOMEZ) in an attempt to locate and arrest YANTHONIC HERRERA, JUNIOR SORIANO FELIX and MAXWELL GOMEZ.

21. Shortly after 3:00 PM, Agents at 1808 Afton Street observed JUNIOR SORIANO FELIX and another male exit the residence and depart the area in FELIX's vehicle. Surveillance units began to follow FELIX but it became apparent that FELIX knew he was being followed.

At that time Agents effected the arrest of FELIX and his passenger. Three cell phones were seized from FELIX at the time of his arrest including iPhone #1 and iPhone #2. During the arrest of FELIX, iPhone #1 was receiving an incoming call and the name "Yan Yan" appeared on the screen as the incoming caller. During a subsequent interview of FELIX, FELIX stated he had been on his way to meet YANTHONIC HERRERA at the time of his arrest. Based upon my knowledge of this investigation, I believe that YANTHONIC HERREA was calling FELIX on iPhone #1.

22. A short time later Agents and Detectives executed a Commonwealth of Pennsylvania search warrant at 1808 Afton Street. Among the items seized was an LTS digital video recorder, the DVR, from the dining room area on the main floor. The DVR was attached to multiple surveillance cameras viewing the area around the exterior of 1808 Afton Street. One of the cameras was pointed at the rear basement door of the residence.

23. Based on my knowledge of this investigation, my training and my experience, I believe the DVR may contain video of HERRERA, FELIX and others engaged in the kidnapping of the victim on July 20, 2019.

24. Agents and Officers attempted to arrest HERRERA later the same day after HERRERA was observed leaving 5945 North Lawrence Street. HERRERA was observed driving his gold Buick Enclave. When Agents attempted to stop HERRERA, HERRERA fled from Agents and Officers in the Buick Enclave. HERRERA eventually left the roadway, drove through a public park and fled on foot from his vehicle into the woods. Agents and Officers were not able to locate HERRERA.

25. A subsequent search of the Buick Enclave resulted in the recovery of iPhone #3. Also recovered from the vehicle was a full case of unused glassine packets identical to those used to package heroin and or fentanyl for street sale.

26. Agents and Officers then obtained and executed a Commonwealth of Pennsylvania search warrant at HERRERA's residence at 7131 Beech Tree Drive, Elkins Park, Pennsylvania. Agents located a heroin/fentanyl packaging operation inside the front bedroom of the apartment. A large amount of both bulk and packaged heroin and fentanyl, packaging material, and other paraphernalia commonly associated with a heroin/fentanyl packaging operation were observed in the front bedroom. Laboratory analysis has determined that the front bedroom contained 5.2 kilograms of fentanyl, 4.6 kilograms of a mixture of fentanyl and heroin, and 118 grams of heroin.

27. Agents also recovered the following items from various locations inside 7131 Beech Tree Drive: iPhone #4, iPhone #5, iPhone #6, the Blackberry, the Alcatel, the MacBook and the Chromebook.

28. On July 29, 2019, the Honorable Thomas J. Rueter issued arrest warrants for YANTHONIC HERRERA and MYRIAM SEVILLA for their involvement in the heroin packaging operation at 7131 Beech Tree Drive. HERRERA and SEVILLA remain fugitives and the FBI is actively trying to locate them.

29. On July 30, 2019, JUNIOR SORIANO FELIX contacted FBI Task Force Officer Greg Oneill. FELIX asked if the FBI would return property which had been seized from him at the time of his arrest including his car keys, cell phones and other personal items. FELIX agreed to come to the Philadelphia FBI Office to reclaim his items.

30. FELIX arrived at the FBI office and expressed a desire to speak with Agents. Agents advised FELIX he was not under arrest, was free to leave at any time and should not discuss anything related to his local arrest on kidnapping charges. FELIX stated he understood and further stated his attorney had advised him not to speak to law enforcement but he wished to do so anyways.

31. FELIX stated he had recently spoken with YANTHONIC HERRERA. FELIX expressed a desire to cooperate with Agents if his cooperation could be used to help HERRERA. Agents explained that HERRERA needed to turn himself in before any arrangement could be considered further. FELIX stated he would attempt to persuade HERRERA to turn himself in.

32. FELIX asked Agents to return his cell phones. SA Wickman agreed to do so if FELIX would provide Agents consent to search the phones. FELIX agreed to allow the search of two phones, one of which is iPhone #2, but denied consent to search iPhone #1, the same phone which had been ringing at the time of his arrest showing the name 'Yan Yan" on the caller ID. Agents visually searched one of FELIX's iPhones and determined the contents to be personal in nature. The iPhone was returned to FELIX. FELIX was unable to recall the password to iPhone #2 and therefore it could not be searched. iPhone #2 was retained by Agents and maintained in FBI evidence storage.

33. FELIX requested to show your affiant something that was stored on iPhone #1. Your affiant provided the phone to FELIX who used a PIN code to unlock the phone. FELIX was careful to shield the PIN code from the view of Agents as he entered it. FELIX opened the Notes application and showed your affiant the screen as FELIX scrolled through numerous Notes entries. FELIX stated that the notes contained information about other drug trafficking organizations in Philadelphia that he would be willing to share with Agents if he could cooperate

on behalf of HERRERA. FELIX then locked the phone and returned it to your affiant. iPhone #1 has been stored in FBI evidence since that time.

34. Based on my training and experience I believe iPhone #1 contains information concerning numerous drug trafficking operations in and around the Philadelphia area. I believe that iPhone #1 may contain information concerning YANTHONIC HERRERA which is not currently known to investigators and may assist Agents in locating HERRERA. I further believe that iPhone #1 may contain information concerning the kidnapping in which both HERRERA and FELIX were participants.

35. On January 11, 2020, MYRIAM SEVILLA was arrested at John F. Kennedy International Airport, Queens, New York. SEVILLA was on an inbound flight originating from the Dominican Republic. SEVILLA was detained by Customs and Border Protection Officers and turned over to the FBI. SEVILLA was in possession of a Samsung SM-J400M cell phone, IMEI 352820102574634, at the time of her arrest.

36. While SEVILLA was undergoing standard post-arrest processing at the FBI JFK Resident Agency, your affiant explained to SEVILLA that she would have an opportunity to cooperate with law enforcement at a later date if she chose to do so. SEVILLA asked your affiant what type of information the FBI believed SEVILLA would be able to provide. Your affiant told SEVILLA that the current location of her boyfriend, YANTHONIC HERRERA, would be of particular importance to the ongoing investigation. SEVILLA responded that she could tell your affiant exactly where HERRERA was.

37. Based on my training and experience, as well as SEVILLA's statement concerning knowing the current location of HERREA, I believe the Samsung cell phone seized

from SEVILLA at the time of her arrest may contain information concerning the current location of fugitive YANTHONIC HERREA.

38. Based on my training and experience, I know that individuals engaged in criminal activity, particularly drug trafficking, utilize their cellular telephones to communicate with co-conspirators to facilitate, plan, and execute their criminal activity and drug transactions. For example, I know that drug traffickers often store contact lists, address books, calendars, photographs, videos, audio files, text messages, call logs, and voice mails on their electronics devices, such as cellular telephones, to be used in furtherance of their criminal activity.

39. Specifically, I know that those involved in drug trafficking communicate with associates using cellular telephones to make telephone calls, send text messages, and communicate via social media platforms. By analyzing call, text, social media and other forms of communications, I may be able to determine the identity of co-conspirators and associated telephone numbers and social media accounts, as well as if there were communications between associates during the commission of crimes.

40. Furthermore, cellular telephones also contain address books with names, addresses, photographs, and phone number of a person's regular contacts. I am aware that drug traffickers frequently list drug associates in directories, often by nickname, to avoid detection by others. Such directories as the ones likely contained on the seized cellular telephones, are one of the few ways to verify the numbers (i.e. telephones) being used by specific traffickers.

41. In addition, I know that those involved with drug trafficking often take photographs or make videos of themselves and their co-conspirators and retain them on their electronic devices such as cellular telephones and computers. This evidence would show associations between accomplices, i.e. photographs of accomplices and/or individuals common

to co-conspirators. I am also aware the drug traffickers often take photographs or make videos of drugs and drug proceeds with their cellular telephones. Based on my training and experience, those who commit these crimes often store these items on their phones to show to associates, in person, via text messaging, and/or via social media.

42. Furthermore, based on my training and experience and the training and experience of other Agents, I know that drug traffickers often use cellular telephone's Internet browser for web browsing activity related to their drug trafficking activities. Specifically, drug traffickers may use Internet search engines to explore where banks or a mail delivery services are located, or may use the Internet to make reservations for travel related to their drug trafficking activities.

43. In addition, drug traffickers sometimes use cellular telephones as a navigation device, obtaining maps and directions to various locations in furtherance of their drug trafficking activities. These electronic devices may also contain GPS navigation capabilities and related stored information that could identify where these devices were located.

44. Furthermore, based on my training and experience, forensic evidence recovered from the review of a cellular telephone can also assist in establishing the identity of the user of the device, how the device was used, the purpose of its use, and when it was used. In addition, I am aware that by using forensic tools, information/data that uses have deleted may still be able to be recovered from the device.

45. Based on my training and experience, I know that computers have the ability to sync information between the computer and a synced cellular telephone. Computers may be used via the internet or installed applications to access cloud data, such as Apple iCloud or Google Drive, which shares information between connected devices such as computer and a

cellular telephone. If cloud data is accessed on an individual's computer, often this data is stored locally on the computer's hard drive. Contact lists, calendar entries, photographs and videos, internet histories, chat and messaging applications and other applications that mirror those used on an individual's cellular telephone are commonly found on an individual's computer. These applications are designed to keep information synced between devices allowing a user to maintain consistent data on whichever device they are using. Computers may contain this type of information for phones which the government has seized as well as for phones the government has not seized.

46. This warrant does not seek to access cloud data stored on a remote server, only data which has been stored locally on the Devices specifically detailed in this warrant.

47. Furthermore, I know that individuals involved in criminal activity often store pictures and documents related to their criminal activity in digital form on their computers. They may also use an internet browser to search for travel information, banking information and other information concerning criminal activity.

48. All of the Devices (iPhone #1, iPhone #2, iPhone #3, iPhone #4, iPhone #5, iPhone #6, the Blackberry, the Alcatel, the Macbook and the Chromebook) are in the lawful possession of the FBI. Therefore, while the FBI might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

49. The Devices are currently in storage at the Philadelphia FBI Field Office. In my training and experience, I know that the Devices have been stored in a manner in which their

contents are, to the extent material to this investigation, in substantially the same state as they were when they first came into the possession of the FBI.

TECHNICAL TERMS

50. Based on my training and experience, I use the following technical terms to convey the following meanings:

51. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

52. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global

Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

53. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

54. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

55. Based on my training, experience, and research, I know that iPhone #1, iPhone #2, iPhone #3, iPhone #4, iPhone #5, iPhone #6, the Blackberry and the Alcatel have capabilities

that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA and have the ability to access the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

56. Digital Video Recorder ("DVR"): A DVR is an electronic device that records video, in a digital format, to a disk drive, flash drive, memory card, or other local or networked mass storage device. DVRs are often used to record video captured by surveillance cameras. DVRs allow a user to review recorded footage captured by a single or network of surveillance cameras. Often times recordings maintained on a DVR contain time and date stamps allowing the identification of when a video was recorded.

57. Based on my training, experience and research, I know that the LTS DVR has the capabilities of a DVR. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence of individuals associating together, an individual's presence at a location at certain dates and times and evidence of an individual's participation in a crime.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

58. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

59. Particularly in reference to the MacBook and Chromebook; There is probable cause to believe that things that were once stored on the MacBook and Chromebook may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

60. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Particularly in reference to the MacBook and Chromebook; Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

c. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

d. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

e. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

f. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

61. *Nature of the examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

62. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

63. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

WILLIAM R. WICKMAN
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on January 31, 2020

HON. RICHARD A. LLORET
United States Magistrate Judge

ATTACHMENT A

1. The property to be searched is:

   a. A rose gold Apple iPhone XS, IMEI 357269098356892, "iPhone #1". The device is passcode protected and additional identifying information is not available in the phone's current state. iPhone #1 is currently located at the Philadelphia Division of the FBI.

   b. A silver Apple iPhone 6, IMEI 352015079785574, "iPhone #2". The device is passcode protected and additional identifying information is not available in the phone's current state. iPhone #2 is currently located at the Philadelphia Division of the FBI.

   c. A LTS digital video recorder, model LTD8304K-ET, serial number 8401804ZUX01512, "DVR". The DVR is currently located at the Philadelphia Division of the FBI.

   d. A silver Apple iPhone 6S, IMEI 354956075078167, "iPhone #3". The device is passcode protected and additional identifying information is not available in the phone's current state. iPhone #3 is currently located at the Philadelphia Division of the FBI.

   e. A silver Apple iPhone 6, IMEI 352013079368335, "iPhone #4". iPhone #4 is currently located at the Philadelphia Division of the FBI.

   f. A gold Apple iPhone 6, IMEI 356148093039706, "iPhone #5". iPhone #5 is currently located at the Philadelphia Division of the FBI.

   g. A silver Apple iPhone 6, IMEI 355786075130026, hereinafter the "iPhone #6". The device is passcode protected and additional identifying information is not

available in the phone's current state. iPhone #6 is currently located at the Philadelphia Division of the FBI.

h. A white Blackberry 9360 Curve, IMEI 35160205611036.2, "Blackberry". The Blackberry is currently located at the Philadelphia Division of the FBI.

i. An Alcatel A521L cell phone, IMEI 014262000754309, "Alcatel". The Alcatel is currently located at the Philadelphia Division of the FBI.

j. An Apple MacBook Air, serial number C02J5TEDDRVC, "MacBook". The MacBook is currently located at the Philadelphia Division of the FBI.

k. A HP Chromebook, serial number 8CG7521XZR, "Chromebook". The Chromebook is currently located at the Philadelphia Division of the FBI.

l. A Samsung SM-J400M cell phone, IMEI 352820102574634, hereinafter the, "Samsung", which was seized from MYRIAM SEVILLA on January 11, 2020 subsequent to her arrest. The Samsung is currently located at the FBI Philadelphia Field Office.

2. This warrant authorizes the forensic examination of the iPhone XS and LTS DVR for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of United States Code, Title 21, Sections 841 and 846 (distribution of and conspiracy to distribute a controlled substance) and United States Code, Title 18, Section 1201 (kidnapping) including:

   a. lists of customers and related identifying information including names, addresses, phone numbers, or any other identifying information;

   b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

   c. any information related to sources of drugs including names, addresses, phone numbers, or any other identifying information;

   d. any information related to methods of trafficking narcotics;

   e. photographs and videos of associates, co-conspirators, and other evidence of drug trafficking;

   f. any information recording domestic and/or international travel or schedules;

   g. any and all information related to credit card bills, account information, and other financial records, including but not limited to, accounts receivable, accounts payable, general ledgers, cash disbursement ledgers, check registers, employment records, and correspondence;

   h. any and all information, including but not limited to, monthly savings and checking statements, banking communications, safe deposit boxes, and wire transfers;

i. stored electronic information and communications, including but not limited to, telephone and address directory entries consisting of names, addresses and telephone numbers, schedule entries, photographs, audio and video.

j. any and all information relating in any way to the possession, sale, purchase, transfer, and/or storage of any and all tangible or intangible assets, including but not limited to, vehicles, real estate, and jewelry regardless of the identity of the person(s) involved;

k. any and all information concerning the purchase, lease, and/or renting of a dwelling or business used as a residence or place to conduct illegal activity;

l. any and all information related to the planning of or the execution of the kidnapping which occurred on July 20, 2019; and

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Any and all information which may lead to the current location of fugitives YANTHONIC HERRERA and MYRIAM SEVILLA.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

5. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government

control) are authorized to review any information removed from the device in order to locate the things particularly described in this Warrant.